Tuesday, June 2

11:10 am – 11:30 am

Operator X: Optimizing Agentic AI for High-Stakes Environments

Nathan Delgado

Director of Software Products

SealingTech

Abstract:

This presentation covers the challenges and evolution of SealingTech's groundbreaking AI platform: Operator X™.

Operator X uses Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG) to enhance the efficiency and effectiveness of the cyber warfighter. To address the unique security requirements of cyber operations, SealingTech prioritizes a fully air-gapped architecture, ensuring that sophisticated agentic capabilities remain effective at the tactical edge without reliance on external connectivity.

To address the Department of War's (DoW) need to operate across a diverse ecosystem of tools, Operator X utilizes the Model Context Protocol (MCP) for agentic workflows. This approach moves away from rigid, one-off integrations toward a flexible architecture enabling a standardized, interoperable bridge between agents and diverse data sources. To facilitate governance in high-stakes environments, Operator X incorporates a human-in-the-loop framework, with live feedback and explained reasoning ensuring oversight of agentic action.

The presentation will share how Operator X continues to evolve and expand its capabilities based on mission needs and a rapidly shifting technology environment. Optimizing Operator X for deployment in disconnected, resource-constrained environments presents significant R&D challenges compared to traditional cloud-enabled AI. Innovations in architecture design, model evaluation, and context window management enable a mobile solution that delivers elite reasoning capabilities at the edge.

By bridging the gap between resource-heavy AI and the disconnected warfighter, SealingTech ensures that defenders can hunt adversaries more effectively and efficiently in any challenging environment.